Smart-1 50/150

Getting Started Guide

Models: S-30, S-40

23 February 2011

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

© 2011 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

Important Information

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=10948

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

Date	Description
23 February 2011	• Added pre-R75 Provider-1/Multi-Domain Security Management terminology ("Multi-Domain Security Management/Provider-1 Terminology" on page 10) • Dedicated SmartEvent Server option available from R75 only ("Security Management Installation Type" on page 21) • Improved formatting and document layout
26 January 2011	• Guide now applies to all Check Point software versions. • Added Rack mounting instructions ("Rack Mounting Smart-1 50/150" on page 12). • Updated the First Time Configuration Wizard Instructions ("Using the First Time Configuration Wizard" on page 19)
26 august 2010	First release of the document

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Smart-1 50/150 Getting Started Guide).

Health and Safety Information

Read the following warnings before setting up or using the appliance.

Warning - Do not block air vents. A minimum 1/2-inch clearance is required.

Warning - This appliance does not contain any user-serviceable parts. Do not remove any covers or attempt to gain access to the inside of the product. Opening the device or modifying it in any way has the risk of personal injury and will void your warranty. The following instructions are for trained service personnel only.

To prevent damage to any system board, it is important to handle it with care. The following measures are generally sufficient to protect your equipment from static electricity discharge:

- When handling the board, to use a grounded wrist strap designed for static discharge elimination.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Handle the board by its edges only. Do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling processor chips or memory modules, avoid touching their pins or gold edge fingers.
- Restore the communications appliance system board and peripherals back into the antistatic bag when they are not in use or not installed in the chassis. Some circuitry on the system board can continue operating even though the power is switched off.
- Under no circumstances should the lithium battery cell used to power the real-time clock be allowed to short. The battery cell may heat up under these conditions and present a burn hazard.

  Warning - DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

- Disconnect the system board power supply from its power source before you connect or disconnect cables or install or remove any system board components. Failure to do this can result in personnel injury or equipment damage.
- Avoid short-circuiting the lithium battery; this can cause it to superheat and cause burns if touched.
- Do not operate the processor without a thermal solution. Damage to the processor can occur in seconds.

For California:

Perchlorate Material - special handling may apply. See http://www.dtsc.ca.gov/hazardouswaste/perchlorate

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5, Chapter 33. Best Management Practices for Perchlorate Materials. This product, part, or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

Proposition 65 Chemical

Chemicals identified by the State of California, pursuant to the requirements of the California Safe Drinking Water and Toxic Enforcement Act of 1986, California Health & Safety Code s. 25249.5, et seq. ("Proposition 65"), that is "known to the State to cause cancer or reproductive toxicity" (see http://www.calepa.ca.gov)

WARNING:

Handling the cord on this product will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Federal Communications Commission (FCC) Statement:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Information to user:

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

Canadian Department Compliance Statement:

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japan Class A Compliance Statement:

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

European Union (EU) Electromagnetic Compatibility Directive

This product is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive (2004/108/EC).

This product is in conformity with Low Voltage Directive 2006/95/EC, and complies with the requirements in the Council Directive 2006/95/EC relating to electrical equipment designed for use within certain voltage limits and the Amendment Directive 93/68/EEC.

Product Disposal

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office or your household waste disposal service.

Contents

Important Information....3
Health and Safety Information....4
Introduction....8
Welcome....8
Smart-1 Overview....8
This document provides:....8
Security Management Software Blades....9
SmartEvent....9
Shipping Carton Contents....9
Terminology....9
SmartEvent Terminology....10
Multi-Domain Security Management/Provider-1 Terminology....10
Rack Mounting Smart-1 50/150....12
Safety Instructions....12
Determining Space and Weight Requirements....12
Rack Mounting Hardware and Tools....13
Disconnecting the Appliance Rail from the Mounting Bracket....14
Attaching the Appliance Rails to the Appliance....15
Attaching the Appliance Handles or Bracket Ears (Optional)....15
Attaching the Mounting Brackets to the Rack....16
Installing Smart 1 50/150 In the Rack....17
Configuring Smart-1....19
Connecting the Power Cables and Power On....19
Using the First Time Configuration Wizard....19
Starting the First Time Configuration Wizard....19
Welcome....20
Appliance Date and Time Setup....20
Network Connections....21
Routing Table....21
DNS and Domain Settings....21
Management Settings....21
Multi-Domain Security Management Settings....24
Installing the SmartConsole GUI Clients....25
Advanced Configuration....26
Connecting to the Smart-1 CLI....26
Migration from Existing Provider-1 Machines....26
Configuring SmartEvent....28
Preparing SmartEvent on Security Management Server....28
Preparing SmartEvent on the Multi-Domain Server....28
Enabling Connectivity with Multi-Domain Security Management....29
Configuring the SmartEvent Clients....29
Defining the Internal Network for SmartEvent....29
Defining Correlation Units and Log Servers for SmartEvent....30
Creating a Consolidation Session for SmartReporter....30
Smart-1 Hardware....31
Smart-1 50 Front Panel....32
Smart-1 150 Front panel....33
LCD Display Screen....33
Customer Replaceable Parts....34
Power Supplies....34
Hard Disk Drives....35
Cooling Fans....37

Restoring Factory Defaults 38
Restoring Factory Defaults using the WebUI 38
Restoring Factory Defaults using the Console 38
Restoring Using the LCD Panel 39
Lights Out Management 41
Introduction 41
Initial Login 41
Basic Configuration Options 42
Remotely Controlling the Appliance 42
Remotely Controlling the Power of the Appliance 42
Managing LOM Card Users 43
Configuring LOM Keyboard/mouse Settings 43
Configuring LOM Settings 44
Setting the Date and Time 44
Defining a LOM Login Message 44
Registration and Support 45
Registration 45
Support 45
Where to From Here? 45

Chapter 1

Introduction

In This Chapter

Welcome	8
Smart-1 Overview	8
Shipping Carton Contents	9
Terminology	9

Welcome

Thank you for choosing Check Point's Smart-1. We hope that you will be satisfied with this solution and our support services. Check Point products provide your business with the most up to date and secure solutions available today.

Check Point also delivers worldwide technical services including educational, professional and support services through a network of Authorized Training Centers, Certified Support Partners and Check Point technical support personnel to ensure that you get the most out of your security investment.

For additional information on the Internet Security Product Suite and other security solutions, refer to the Check Point Web site (http://www.checkpoint.com), or call Check Point at 1(800) 429-4391. For additional technical information about Check Point products, consult the Check Point Support Center (http://supportcenter.checkpoint.com).

Welcome to the Check Point family. We look forward to meeting all of your current and future network, application and management security needs.

Smart-1 Overview

Smart-1 appliances deliver Check Point's market leading security management software blades on a dedicated hardware platform specifically designed for mid-size and large enterprise security networks. Based upon Check Point's software blade architecture, Smart-1 appliances deliver a unified management solution for network, IPS and endpoint security with unsurpassed extensibility.

- Provides a comprehensive set of security management Software Blades
- Maximize efficiency with a single unified management console for network and endpoint security
- Reduce costs and conserve resources with up to 12 TB of built-in storage capabilities
- Ensure operational continuity for the most demanding environments
- Simplify large scale security policy provisioning with Multi-Domain Security Management (Provider-1)

This document provides:

- A brief overview of essential Smart-1 concepts and features
- A step by step guide to getting Smart-1 up and running

Note - Screen shots in this guide may apply only to the highest model to which this guide applies.

Security Management Software Blades

Smart-1 Appliances includes the following Security Management Software Blades:

- Network Policy Management
- Endpoint Policy Management
- Logging & Status
- SmartProvisioning
- Monitoring
- User Directory
- Management Portal
- SmartEvent (IPS Event Analysis, Reporting and Event Correlation)
- Multi-Domain Security Management

SmartEvent

Smart-1 includes SmartEvent, which is made up of IPS Event Analysis, Reporting and Event Correlation. SmartEvent provides centralized reporting and real-time security event correlation and management of your security data. Security teams no longer need to comb through the massive amount of data generated by the devices in their environment. Instead, they can focus on deploying resources on the important threats and trends that pose the greatest risk to their business.

You can configure Smart-1 as a Security Management server with SmartEvent. In R75 and higher, you can also configure Smart-1 as a dedicated server for SmartEvent.

Shipping Carton Contents

Item	Description
Appliance	A single Smart-1 appliance
Rack Mounting Accessories	Hardware mounting kit
Cables	• 2 power cables (Smart-1 50) 3 power cables (Smart-1 150) • 1 standard LAN cable • 1 serial console cable
Documentation	• User license agreement • Quick Start Guide • Getting Started Guide

Terminology

The following Smart-1 terms are used in this guide:

- **Security Gateway**: The security engine that enforces the organization’s security policy and acts as a security enforcement point.
- **Security Policy**: The policy created by the system administrator that regulates the flow of incoming and outgoing communication.

- **Security Management server**: The server used by the system administrator to manage the security policy. The organization's databases and security policies are stored on the Security Management server and downloaded to the gateway. Smart-1 is a Security Management server.
- **SmartConsole**: GUI applications that are used to manage various aspects of security policy enforcement. For example, SmartView Tracker is a SmartConsole application that manages logs.
- **SmartDashboard**: A SmartConsole GUI application that is used by the system administrator to create and manage the security policy.
- **Management High Availability (HA)**: Refers to a configuration in which a primary Security Management server has one or more backup secondary Security Management servers which are ready to take over in case of failure of the primary Security Management server.

SmartEvent Terminology

- **SmartEvent and Reporter Suite:** Includes SmartEvent and SmartReporter.
  - **SmartEvent:** A system that reads logs and generates events based on an Event Policy. An IPS event-only version is also available. Based on the configuration, SmartEvent contains these components:
    - **SmartEvent Client** (or **IPS Event Analysis Client**)**:** A GUI that displays events (or IPS events) in many graphical, list and map forms and provides user control of the policy.
    - **SmartEvent Server** (or **IPS Event Analysis Server**)**:** Holds the event (or IPS event) database, event queries, object values and policy definition.
    - **SmartEvent Correlation Unit:** An engine which reads logs and creates events.
  - **SmartReporter:** A system that reads logs and generates statistical and data reports. SmartReporter contains these components:
    - **SmartReporter Client:** A GUI to generate, define and display reports.
    - **SmartReporter Server:** Contains reports, report definitions and report schedules.
    - **Log Consolidator:** Reads logs, consolidates them according to the consolidation policy and adds them to the SmartReporter database.

Multi-Domain Security Management/Provider-1 Terminology

The following terms relate to **Multi-Domain Security Management**:

- **Multi-Domain Server**: The Multi-Domain Server houses Multi-Domain Security Management system information including details of the Multi-Domain Security Management deployment, its administrators and customer management datum. There are two Multi-Domain Server types: the Manager, which runs the Multi-Domain Security Management deployment, and the Container, which holds the Domain Management Server. The Manager is the administrator's entry point into the Multi-Domain Security Management environment. A Multi-Domain Server can be a Manager, a Container, or both.
- **Domain Management Server**: The Multi-Domain Security Management equivalent of the Security Management Server for a single customer. Through the Domain Management Server, an administrator creates security policies and manages the customer gateways.
- **SmartDomain Manager**: The primary interface used to handle customer security management by Multi-Domain Security Management administrators. The SmartDomain Manager is used to update Customer and gateway information, and to assign and navigate between global policies.

Changes in Multi-Domain Security Management/Provider-1 Terminology

These product names changed starting with R75. The changed names are used throughout this guide:

Name Before R75	Name Starting with R75 (Used in this Guide)
Provider-1	Multi-Domain Security Management
Provider-1 MDG	SmartDomain Manager

Name Before R75	Name Starting with R75 (Used in this Guide)
Multi-domain server (MDS)	Multi-Domain Server
Customer	Domain
Customer Management Add-on (CMA)	Domain Management Server
Customer Log Module (CLM)	Domain Log Server
Multi-Domain Log Module (MLM)	Multi-Domain Log Server

Chapter 2

Rack Mounting Smart-1 50/150

These instructions show how to install Smart-1 50 and 150 in a standard 19 inch rack.

In This Chapter

Safety Instructions 12
Determining Space and Weight Requirements 12
Rack Mounting Hardware and Tools 13
Disconnecting the Appliance Rail from the Mounting Bracket 14
Attaching the Appliance Rails to the Appliance 15
Attaching the Appliance Handles or Bracket Ears (Optional) 15
Attaching the Mounting Brackets to the Rack 16
Installing Smart 1 50/150 In the Rack 17

Safety Instructions

Before installing your appliance in a rack cabinet, review the following guidelines:

- Make sure that the room air temperature is below 35°C (95°F).
- Do not block any air vents. Normally, 15 cm (6 in.) of air space in the rear and 5 cm (2 in.) in the front provides proper airflow.
- Install the appliances in the cabinet starting at the bottom and going up.
- Install the heaviest appliance at the bottom of the rack cabinet.
- Do not extend more than one device out of the rack cabinet at the same time.
- Connect the server to a properly grounded outlet.
- Do not overload the power outlet when installing multiple devices in the rack cabinet.

Determining Space and Weight Requirements

Allow sufficient vertical space in the rack for the appliance:

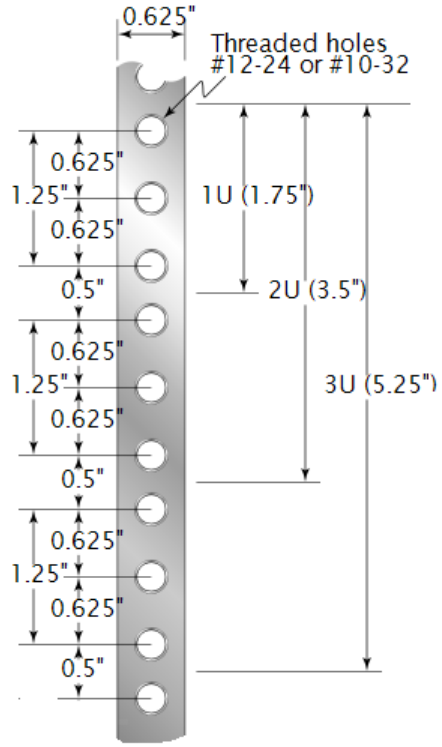
Model	Height	Weight (Kg)
Smart-1 50	2U (3.5 inch , 88.9 mm)	28
Smart-1 150	3U (5.25 inch, 133.3 mm)	38

Important - The Smart-1 appliance is very heavy. To lift and install it:

- Two people are required for Smart-1 50.
- Three people are required for Smart-1 150.

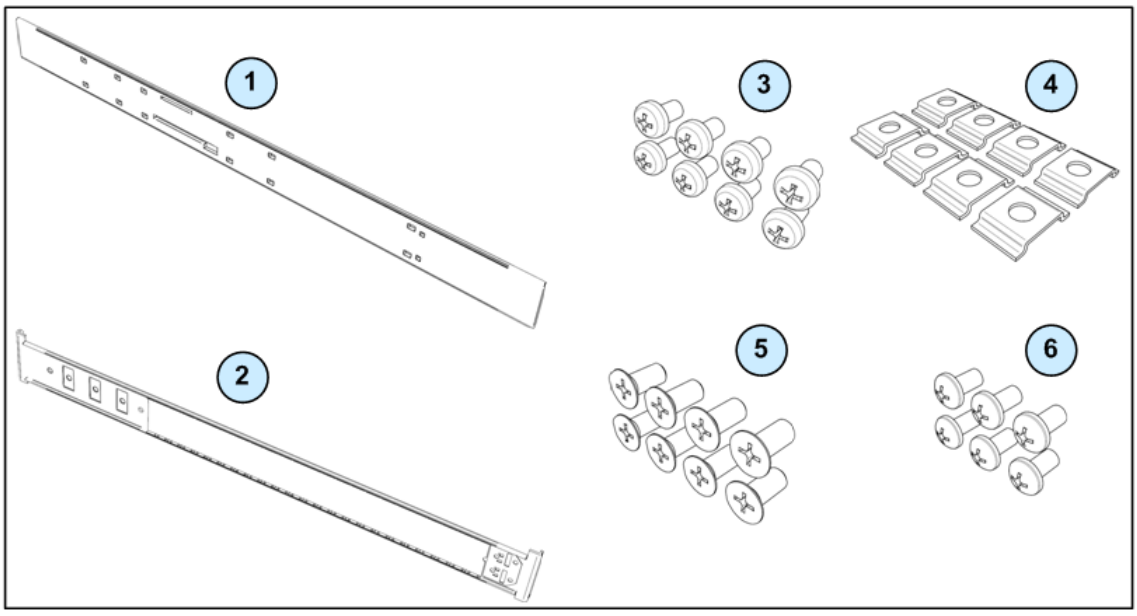
The distance from the center of any hole to the center of the third hole above it is equivalent to 1U.

The mounting holes in a standard 19-inch (482.6 mm) server rack rail are arranged as follows:



When installing appliances, start measuring from the center of the two holes with closer spacing. Otherwise, the screw holes on the appliance may not match those on the rack.

Rack Mounting Hardware and Tools



Key	Description	Qty.	Use
(1)	Appliance rail	2	Attaches to the Smart-1 50/150 appliance. Both rails are identical.
(2)	Mounting Bracket	2	Attaches to the rack vertical rails. Both brackets are identical.
(3)	Screws for Rack Mounting	8	Secures the mounting bracket to the rack vertical rails
(4)	Square washers for rack mounting screws	8	Secures the mounting bracket to the rack vertical rails.
	Round washers for rack mounting screws	8	Secures the mounting bracket to the rack vertical rails
(5)	Screws for Smart-1 50 M3*6	8	Secures the appliance rail to Smart-1 50
(6)	Screws for Smart-1 150 #6-32*6	6	Secures the appliance rail to Smart-1 150
	Appliance bracket ear for Smart-1 50	2	Attaches to the Smart-1 50 front panel. Both bracket ears are identical.
	Screw for Smart-1 50 appliance bracket ear	6	Attaches the Smart-1 50 bracket ears to the appliance
	Handle for Smart-1 150	2	Attaches to the Smart-1 150 front panel. Both handles are identical.
	Screw for Smart-1 150 handle	4	Attaches the Smart-1 150 handles to the appliance

Rack Mounting Tools

- Philips screwdriver. A magnetic head is recommended to hold screws in place and retrieve dropped screws. A powered screwdriver is useful.

Disconnecting the Appliance Rail from the Mounting Bracket

Disconnect the appliance rail from the mounting bracket.

You don't need to do this in the server room.

1. Fully extend the combined appliance rail and mounting bracket.

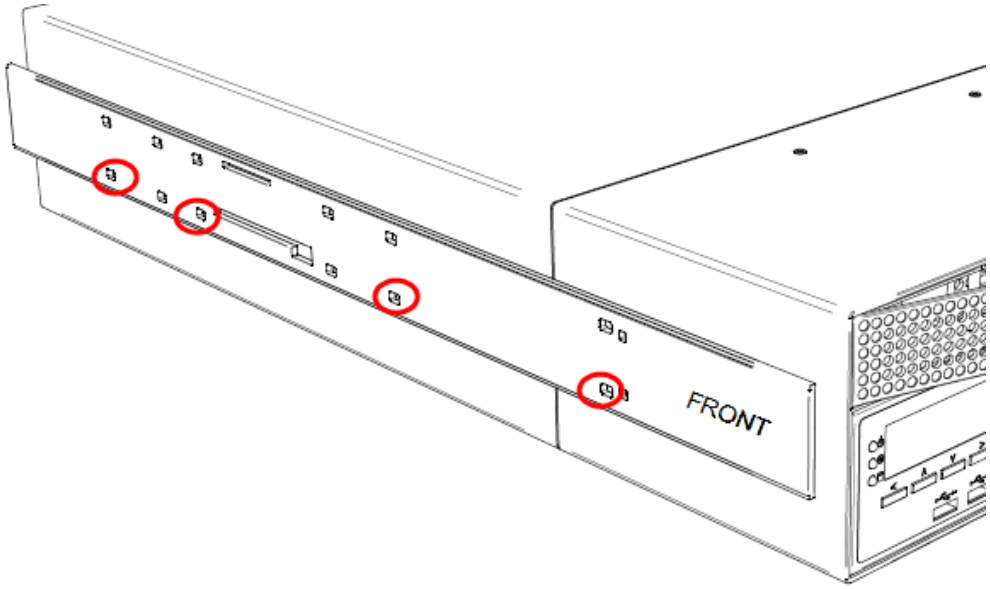
2. Press plastic release catch in the direction of the arrow to disconnect the appliance rail from the mounting bracket.

Attaching the Appliance Rails to the Appliance

Attach the Appliance Rails to the Appliance. Use the same appliance rails for Smart-1 50 and for Smart-1 150.

You don't need to do this in the server room.

1. Identify the front of an appliance rail. One end of the rail is marked with FRONT.
2. Position the appliance rail on the side of the appliance:
   a) Line up the front end of the rail with the front panel of the appliance,
   b) Slide the appliance rail backwards until the correct holes in the appliance rail line up with the holes in the side of the appliance:
      - On the Smart-1 50, line up the four holes marked 50 with the holes in the appliance.



      - On the Smart-1 150, line up the three holes marked 150 with the holes in the appliance.
3. Attach the appliance rail to the side of the Smart-1 appliance.
   - For Smart-1 50 use four M3*6 screws
   - For Smart-1 150 use three #6-32*6 screws
4. Repeat for the other side of the appliance.

Attaching the Appliance Handles or Bracket Ears (Optional)

The appliance ear bracket (for Smart-1 50) and the appliance handles (for Smart-1 150) are optional. Use them as a

- Handle, to make it easier to grab the front of appliance and slide it in and out. The Smart-1 150 is very heavy. You can use the handles to help move and lift the appliance.
- Buffer that prevents to appliance jamming in the rack in the closed position.

You can also use the appliance ear brackets to prevent the appliance from sliding in and out of the rack, by attaching the bracket ears to the rack vertical rail.

You don't need to be in the server room to attach the appliance handles or ear brackets to the appliance.

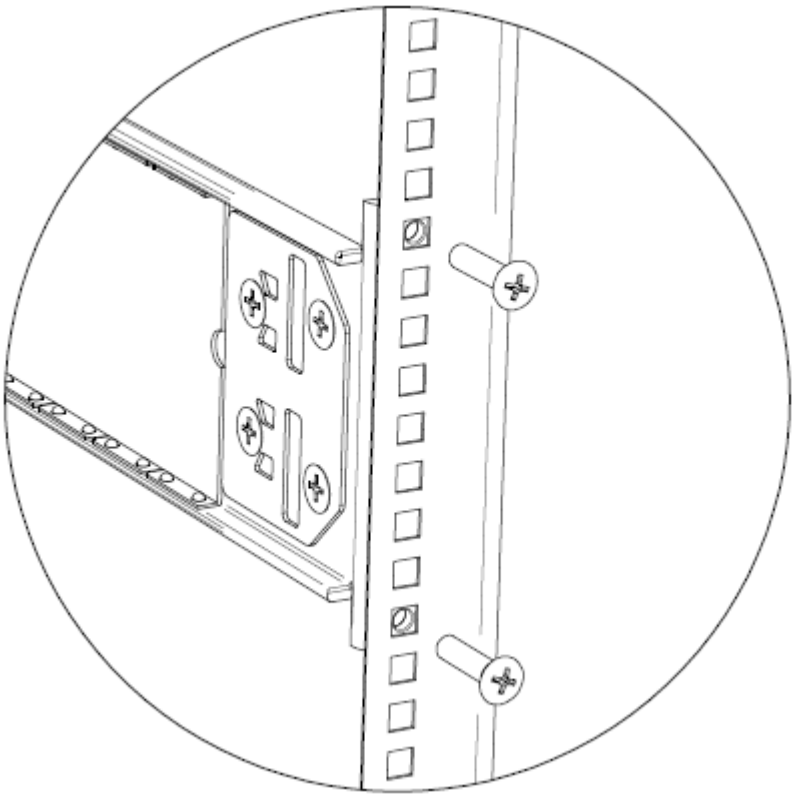
To connect the appliance bracket ears or handles to the front of the appliance:

1. Attach the appliance ear bracket to one side of the appliance. For Smart-1 50 use three screws. For Smart-1 150 use two screws.
2. Repeat for the other side of the appliance.

Attaching the Mounting Brackets to the Rack

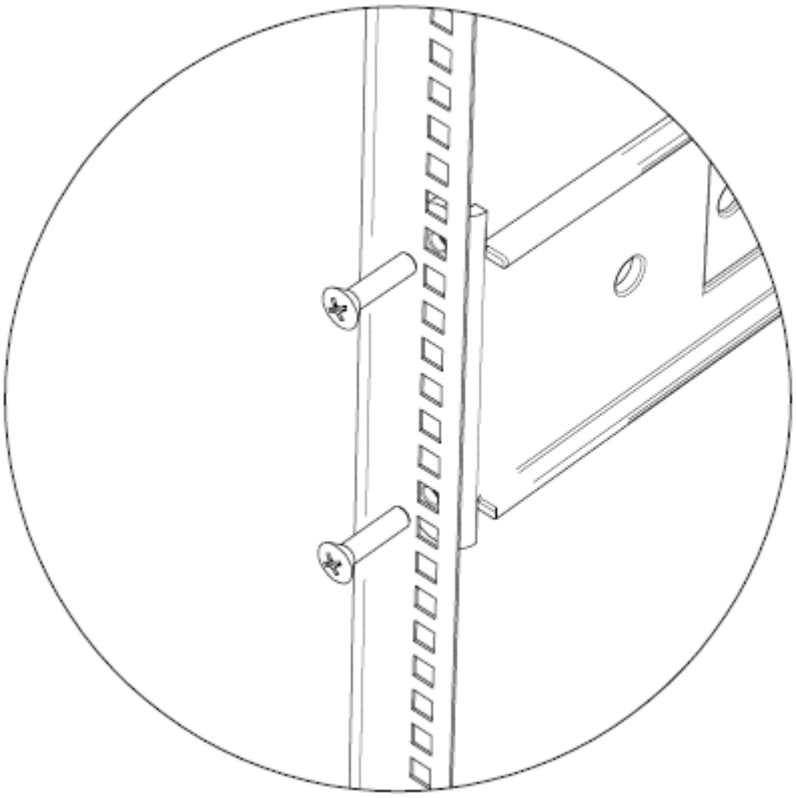
Attach the mounting brackets to the rack:

1. While standing in the front of the rack, place a mounting bracket in position on one side of the rack
2. Attach the mounting bracket to the rack vertical rail at the front using two screws:
   a) Place a round washer on a rack mounting screw, then a square washer
   b) Attach the mounting bracket to the rack vertical rails using the screw and washers. For now, do not fully tighten the screw.
   c) Repeat for the second screw.



3. Go to the back of the rack.

4. Attach the mounting bracket to the rack vertical rail at the back using the same number of screws and washers. Tighten the two screws normally.



5. Go the front of the rack.
6. Tighten the two screws that attach the mounting bracket to the rack vertical rail.
7. Repeat for the other side of the rack: Attach the mounting bracket to the other side of the rack.

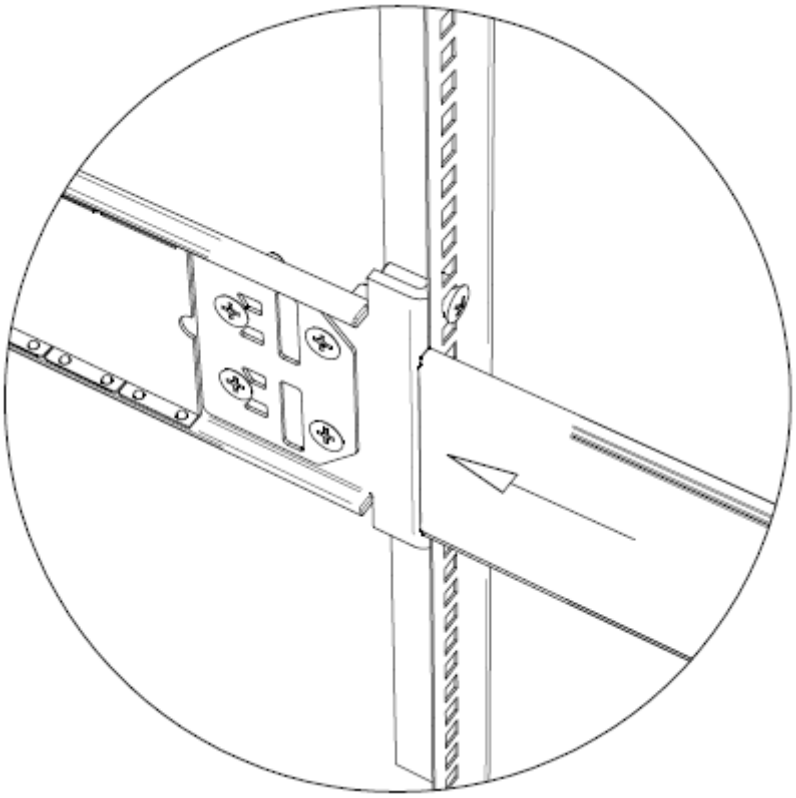
Installing Smart 1 50/150 In the Rack

Carefully install the Smart-1 50/150 in the rack.

Important - The Smart-1 appliance is very heavy. To lift and install it:

- Two people are required for Smart-1 50.
- Three people are required for Smart-1 150.

1. Line up the appliance rail on the appliance with the mounting bracket rails.



2. Carefully slide the appliance into the mounting bracket rails.
3. Push the appliance in until the appliance locks in the rails.

Chapter 3

Configuring Smart-1

The basic workflow for configuring Smart-1 is:

1. Connect the cables and power on.
2. Perform the initial configuration using the First Time Configuration Wizard.
3. Install the SmartConsole GUI clients.

In This Chapter

Connecting the Power Cables and Power On	19
Using the First Time Configuration Wizard	19
Installing the SmartConsole GUI Clients	25
Advanced Configuration	26
Migration from Existing Provider-1 Machines	26

Connecting the Power Cables and Power On

1. Connect the power cable(s).
2. Turn on the Power button to start the appliance.

Note - When a power supply fails or is not connected to the outlet, an alarm sounds continuously. If you hear the alarm, check that all power supplies are connected to the outlets. If needed, replace the faulty power supply immediately, and connect the new unit to the A/C outlet. See "Removing the Power Supply (on page 35)".

Using the First Time Configuration Wizard

Perform the initial configuration of Smart-1 using the First Time Configuration Wizard.

At any time you can click **Quit** to exit the wizard. Click **Next** to move to the next page.

Note - When running the First Time Configuration Wizard, you may not see all the pages shown in this section of the guide, and they may not appear in the order shown. The pages that appear in the wizard and their order depend on the Smart-1 software image and on the selections you make.

Starting the First Time Configuration Wizard

1. Connect a standard network cable to the appliance's management interface and to your management network.

The management interface is marked **Mgmt**. This interface is preconfigured with the IP address 192.168.1.1.

2. Connect to the management interface by connecting from a computer on the same network subnet as the management interface (for example, with IP address 192.168.1.x and netmask 255.255.255.0). This can be changed later through the management interface.
3. To access the administration interface, initiate a connection from a browser to the default administration IP address: https://192.168.1.1:4434.

Note - Pop-ups must always be allowed on `https://<appliance_ip_address>`.

The login page appears.

4. Log in with the default system administrator login name/password: **admin/admin**, and click **Login**.
5. The **First-Time Configuration Wizard** runs. The Wizard presents a number of windows, in which you are prompted to configure Smart-1.

Note - The features configured in the wizard are accessible after completing the wizard via the WebUI menu. The WebUI menu can be accessed by navigating to https://<appliance_ip_address>:4434.

Welcome

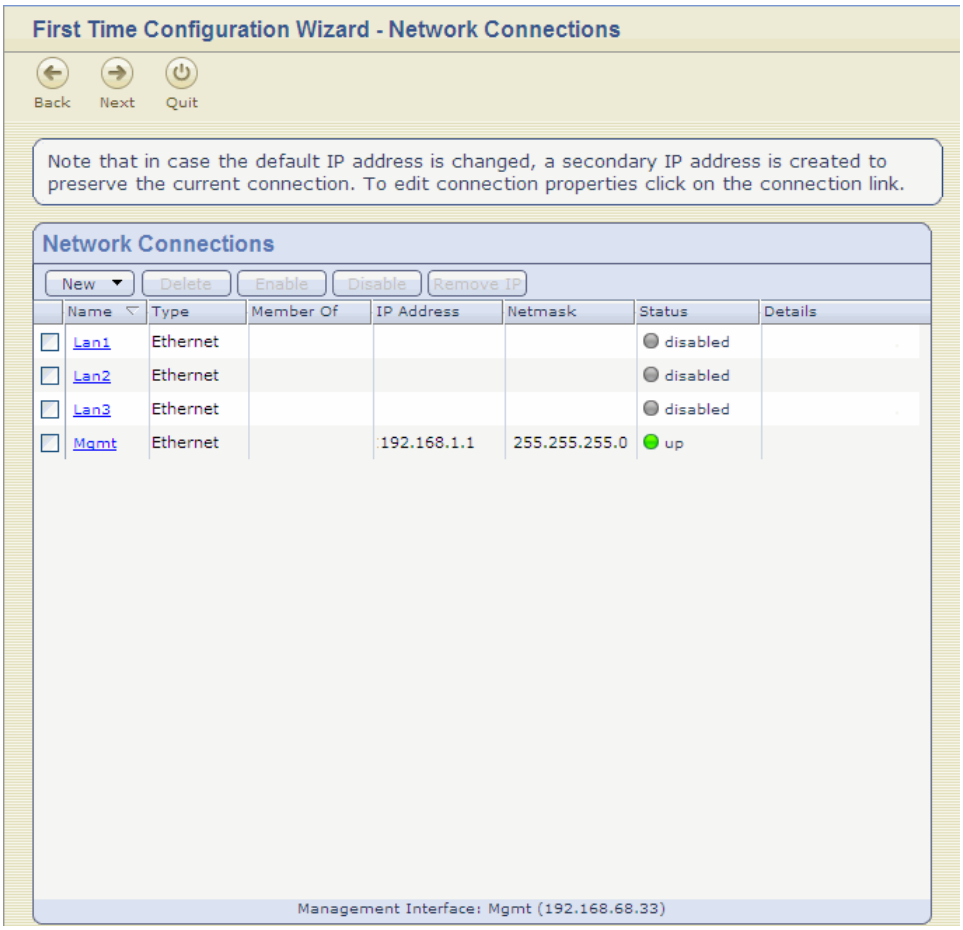
The **Welcome** page summarizes the steps of the First Time Configuration Wizard.

Appliance Date and Time Setup

Configure date and time in the **Date and Time Setup** page. Click **Apply**.

Network Connections

Configure Network Connections in the **Network Connections** page.



You may modify the Mgmt IP address and connectivity will be preserved. A secondary interface is created automatically to preserve connectivity. This interface can be removed after the wizard is completed in the **Network** > **Network Connections** page.

Routing Table

Configure Routing on the **Routing Table** page.

DNS and Domain Settings

Set the Host, Domain and DNS Servers in the **DNS and Domain Settings** page.

The host name must start with a letter and cannot be named Com1, Com2, … , Com9.

Management Settings

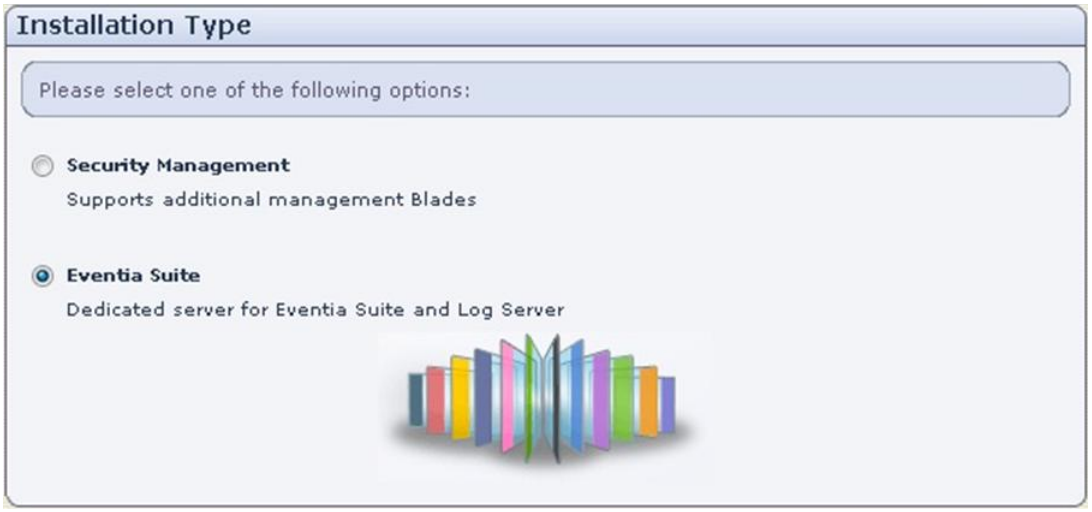
The remaining screens of the First Time Configuration Wizard are specific to the image you have on the Smart-1

- If Smart-1 has a Security Management server image, continue with the screens in this section.
- If Smart-1 has a Multi-Domain Security Management image, continue with the Multi-Domain Security Management settings (on page 24).

Security Management Installation Type

Note - This page is only available in R75 or higher.

In the **Installation Type** page:


Installation Type
Please select one of the following options:
Security Management
Supports additional management Blades
Eventia Suite
Dedicated server for Eventia Suite and Log Server

- **Security Management:** Configure Smart-1 as a Security Management server with all the management Software Blades, including SmartEvent.
- **Eventia Suite** (SmartEvent and Reporter Suite): Configure Smart-1 as a dedicated server for SmartEvent, and no other Software Blade. SmartEvent and Reporter Suite contains SmartReporter Server, SmartEvent Server, and SmartEvent Correlation Unit.

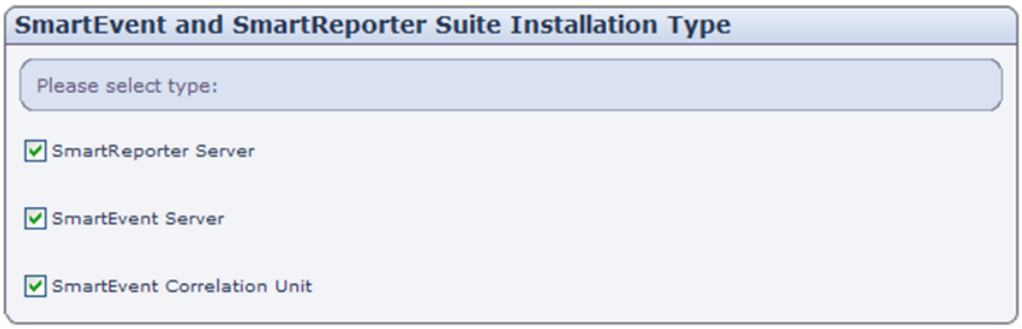
Security Management

If you choose to install a Security Management server, in the **Security Management** page:

- **Primary Security Management** is the Security Management server that will normally be active. To set up a Security Management server in a non-Management HA deployment, choose this option. In a Management HA deployment, if the Primary Security Management server fails, the Secondary Security Management server takes over.
- **Secondary Security Management** is the Security Management server that takes over if the Primary Security Management server fails. This option applies only in a Management HA deployment.
- **Log Server** is the repository for log entries generated on gateways. Check Point gateways send their log entries to the Log Server.

SmartEvent and SmartReporter Suite Installation Type

Configure the SmartEvent and Reporter Suite applications to run on the server.



SmartEvent: A system that reads logs and generates events based on an Event Policy. An IPS event-only version is also available. **SmartReporter** is a system that reads logs and generates statistical and data reports. Choose one or more of these server components:

- **SmartReporter Server:** Contains reports, report definitions and report schedules.
- **SmartEvent Server:** Holds the event (or IPS event) database, event queries, object values and policy definition.
- **SmartEvent Correlation Unit:** An engine which reads logs and creates events.

For IPS Event Analysis, select both **SmartEvent Server** and **SmartEvent Correlation Unit**.

Web/SSH and GUI Clients Configuration

Define the clients that are allowed to connect to the Smart-1 appliance using a Web browser, SSH client, or SmartConsole applications.

You can define a **Host** according to **Hostname** or **IP address**. Enter `Any` to manage Smart-1 from anywhere.

Note - It is not recommended to use the `Any` value for security reasons.

Additional options are available via the **WebUI** menu, after you complete the First Time Configuration Wizard.

Secure Internal Communication

In the **Secure Internal Communication** page, enter a SIC Activation Key and remember it, as you will enter it again when configuring the object via SmartDashboard.

Download SmartConsole Applications

Configuring a security policy requires you to install the SmartConsole applications. In the **Download SmartConsole Applications** window, you can download SmartConsole and install it on Windows machines. For a detailed list of supported Windows operating systems for SmartConsole refer to the release notes of your Check Point version in the Check Point Support Center (http://supportcenter.checkpoint.com).

Summary

The **Summary** page appears.

Click **Finish** to complete the First-Time Configuration Wizard. The Appliance will automatically restart. This may take several minutes.

Note - It is recommended to backup the system configuration for system recovery purposes. The backup menu can be accessed via the WebUI interface under the **Appliance** menu.

Multi-Domain Security Management Settings

The First Time Configuration Wizard screens in this section apply to a Smart-1 with a Multi-Domain Security Management image.

Note - This section uses terminology introduced in R75 ("Multi-Domain Security Management/Provider-1 Terminology" on page 10). The instructions apply to all software versions.

Web and SSH Clients

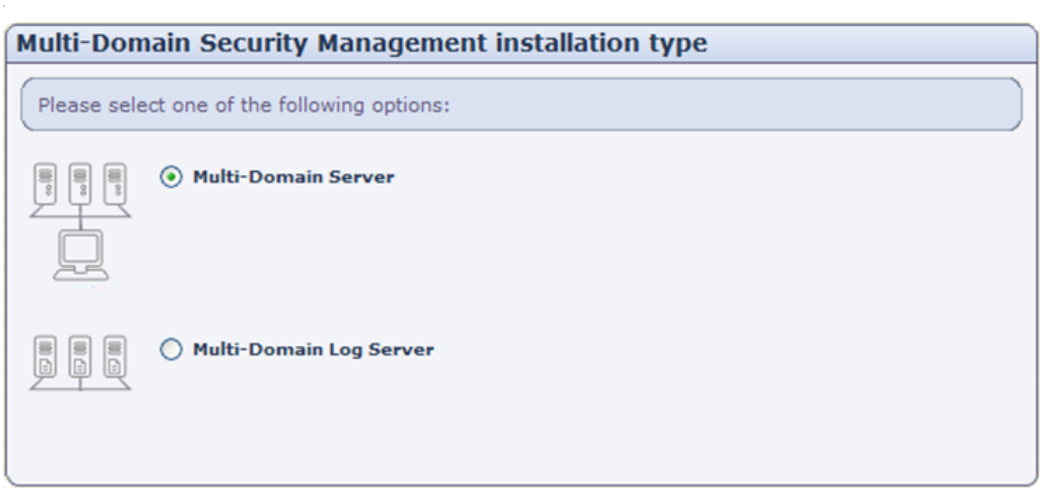
Define the clients that are allowed to connect to the Smart-1 appliance using a Web browser, SSH client, or SmartConsole applications.

You can define a **Host** according to **Hostname** or **IP address**. Enter `Any` to manage Smart-1 from anywhere.

Note - It is not recommended to use the `Any` value for security reasons.

Additional options are available via the **WebUI** menu, after you complete the First Time Configuration Wizard.

Multi-Domain Security Management Installation Type


Multi-Domain Security Management installation type
Please select one of the following options:
Multi-Domain Server
Multi-Domain Log Server

- **Multi-Domain Server:** select this option if you want the appliance to house Multi-Domain Security Management system information including details of the Multi-Domain Security Management deployment, its administrators and customer management datum. There are two Multi-Domain Server types: the Manager, which runs the Multi-Domain Security Management deployment, and the Container, which holds the Domain Management Server. The Manager is the administrator's entry point into the Multi-Domain Security Management environment. A Multi-Domain Server can be a Manager, a Container, or both.
- **Multi-Domain Log Server:** select this option if you want the appliance to host your Domain Log Server (virtualized log servers).

Multi-Domain Server Configuration

Multi-Domain Server configuration
Please select one of the following options:
Primary Multi-Domain Server
This is the first Multi-Domain Server machine I am installing in my environment.
Secondary Multi-Domain Server
I have another Multi-Domain Server in my environment, already configured to be the Primary Multi-Domain Server.

- **Primary Multi-Domain Server** is the Multi-Domain Server that will normally be active. To set up an Multi-Domain Server in a non-High Availability deployment, choose this option. In a High Availability deployment, if the Primary Multi-Domain Server fails, a Secondary Multi-Domain Server will be available to resume management tasks.
- **Secondary Multi-Domain Server** is an Multi-Domain Server that may also be used if the Primary Multi-Domain Server fails.

Multi-Domain Security Management Administrator

Define the clients that are allowed to connect to the Smart-1 appliance using the SmartDomain Manager.

Secure Internal Communication

In the **Secure Internal Communication** page, enter a SIC Activation Key and remember it, as you will enter it again when configuring the object via SmartDashboard.

Download SmartConsole Applications

Configuring a security policy requires you to install the SmartConsole applications. In the **Download SmartConsole Applications** window, you can download SmartConsole and install it on Windows machines. For a detailed list of supported Windows operating systems for SmartConsole refer to the release notes of your Check Point version in the Check Point Support Center (http://supportcenter.checkpoint.com).

Summary

The **Summary** page appears.

Click **Finish** to complete the First-Time Configuration Wizard. The Appliance will automatically restart. This may take several minutes.

Note - It is recommended to backup the system configuration for system recovery purposes. The backup menu can be accessed via the WebUI interface under the **Appliance** menu.

Installing the SmartConsole GUI Clients

1. The WebUI menu can be accessed by navigating to https://<appliance_ip_address>:4434.
2. Login using the administrator username and password configured in step 4 of the Advanced Initial Configuration step.
3. Download the SmartConsole Installation package **Product Configuration > Download SmartConsole > Download**.

4. If Multi-Domain Security Management is deployed, follow the same procedure to download the SmartDomain Manager.

You have now completed the Smart-1 configuration.

To start working with your Smart-1 appliance as a Security Management Server refer to the *Security Management Server Administration Guide*.

To start working with your Smart-1 appliance as Multi-Domain Security Management, refer to the *Multi-Domain Server Administration Guide*.

Advanced Configuration

Advanced configuration can be done using the `sysconfig` or `mdsconfig` menu which can be accessed using the command line interface only.

Note - The `sysconfig` menu is only available after running the **First Time Configuration Wizard** in the WebUI.

Command line access can be obtained by console connection or through SSH.

Connecting to the Smart-1 CLI

You can connect to the command line interface of the Smart-1 appliance using:

- The provided serial console cable (DTE to DTE) and terminal emulation software such as HyperTerminal (from Windows) or Minicom (from Unix/Linux systems).

  Connection parameters for Smart-1 appliances are: 9600bps, no parity, 1 stop bit (8N1).
- An SSH connection to the management interface (if sshd is configured).

Migration from Existing Provider-1 Machines

Smart-1 introduces a simple and easy to use tool that enables migration from existing NGX R65 and higher Provider-1 machines into the Smart-1 appliance.

This script exports the entire existing MDS database into one .tgz file on the source machine that can be imported to the Smart-1 machine.

To migrate from an existing NGX R65 and higher Provider-1 machine into the Smart-1 appliance:

Before starting the migration:

The exported configuration is approximately the size of the MDS installation. Therefore, before starting the migration make sure you have enough free disk space on the source and target machines.

On the source machine:

1. Get the `p1_upgrade_tools.tgz` package (http://supportcontent.checkpoint.com/solutions?id=sk43266).
2. Extract the package contents
3. Run the export_mds.sh tool (make sure it has executable permissions)

```
# export_mds.sh <path to store exported mds configuration>
```

On the Smart-1 appliance:

1. Verify that no customers are defined, and that there are no global objects and policies on the Smart-1 machine. Administrators and/or GUI clients will be overwritten.
2. Transfer the exported mds file to the `/var` partition on the Smart-1 machine.
3. Run the import tool:

```
# $MDS_SYSTEM/install/mds_import.sh <full path to the imported configuration>
```

4. Start the mds.
   Note that the first start-up of the mds after import takes considerably longer than subsequent start-ups.

Chapter 4

Configuring SmartEvent

This section explains how to get up and running with SmartEvent.

In This Chapter

Preparing SmartEvent on Security Management Server 28
Preparing SmartEvent on the Multi-Domain Server 28
Enabling Connectivity with Multi-Domain Security Management 29
Configuring the SmartEvent Clients 29

Preparing SmartEvent on Security Management Server

To configure SmartEvent, first establish connectivity between the components.

1. Launch SmartDashboard.
2. In SmartDashboard, create a new host for each computer that contains a component of SmartEvent:
   a) Select **Manage > Network Object > New > Check Point > Host**
   b) In the **General Properties** window, click **Communication** and enter the activation key.

   Note - If the Security Management Server and SmartEvent are installed on different sides of the firewall, add a rule that allows SIC traffic between them.

   c) The version is not entered automatically if the SmartEvent version is newer than the version of the Security Management Server. If so, select the most recent version available from the **Version** drop-down list.
   d) In the **Management Software Blades** list, select the blades that are installed on the new host.
3. Install the database on all log servers from which SmartEvent reads data: select **Policy > Install Database** and select the log servers as the targets.
4. To allow the SmartEvent Intro server to block attacks from specific IP addresses, configure the Security Management Server to accept SAM commands from the SmartEvent Intro server:
   a) On the Security Management Server, edit the `$CPDIR/conf/sic_policy.conf` file:

   Search for the section `[Inbound rules]`, and add the following line under `# sam proxy`:

   ```
   DN_Mgmt ; Reporting_Tool; ANY; sam ; sslca
   ```

   b) From the command line in the Security Management Server computer, run the following commands:
   ```
   cpstop
   cpstart
   ```

Preparing SmartEvent on the Multi-Domain Server

The first stage configuring SmartEvent is to establish connectivity between the components.

1. Launch Global SmartDashboard.

2. In SmartDashboard, create a new host for each computer that contains a component of SmartEvent:
   a) Select **Manage > Network Object > New > Check Point > Host**
   b) In the **General Properties** window, click **Communication** and enter the activation key.

   Note - If the Multi-Domain Server and SmartEvent are installed on different sides of the firewall, add a rule that allows SIC traffic between them.

   c) The version is not entered automatically if the SmartEvent version is newer than the version of the Multi-Domain Server. If so, select the most recent version available from the **Version** drop-down list.
   d) In the **Management Software Blades** list, select the blades that are installed on the new host.
3. Select **Close** and **OK**.
4. From the **File** menu, select **Save**.
5. From the SmartDomain Manager:
   a) Do **Install Global Policy** on all CMAs participating with SmartEvent.
   b) For each CMA participating with SmartEvent, open its SmartDashboard, select **Policy > Install Database**, and select only the Log Servers and the CMA from which you want the SmartEvent Intro or SmartReporter components to read logs.

Enabling Connectivity with Multi-Domain Security Management

1. Open the SmartEvent Intro client, go to **Policy tab > General Settings > Objects > Customers**, and add all the CMAs with which you will be working.
2. Objects will be synchronized from the CMAs. The synchronization progress can be monitored from the status window in the **Overview** pane.

Configuring the SmartEvent Clients

You must perform these configurations to make the components of the SmartEvent functional.

After you have accomplished the tasks for SmartEvent Intro, events will begin to appear in the SmartEvent Intro client.

After you have accomplished the tasks for SmartReporter, logs will be created and sent to the SmartReporter database. Reports can then be created.

Defining the Internal Network for SmartEvent

To help SmartEvent Intro determine whether events originated internally or externally, the Internal Network must be defined. Certain network objects are copied from the management server to the SmartEvent Intro server during the initial synchronization and updated afterwards periodically. Define the Internal Network from these objects.

Note - If running IPS Event Analysis in a Security Management Server environment, the internal network will be defined automatically from firewall topology information. You can customize the internal network definition.
In a Multi-Domain Security Management environment, define an internal network for each CMA.

To define the Internal Network:

1. Start the SmartEvent Intro Client.
2. From the **Policy** view, select **General Settings > Initial Settings > Internal Network**.
3. Add objects (hosts, networks, groups, IP ranges) that define your environment's internal network.

Defining Correlation Units and Log Servers for SmartEvent

1. From the **Policy** view of the SmartEvent Intro client, select **General Settings > Initial Settings > Correlation Units**.
2. Select **Add**.
3. Click the button of the **Correlation Unit** field.
4. In the **Select Objects** window, select a Correlation Unit.

   Note - In a Multi-Domain Security Management environment, add the log servers for each CMA.
5. Click **OK**.
6. Click **Add** and select the Log Servers available as data sources to the Correlation Unit.
7. Select **Save**.
8. From the **Actions** menu, select **Install Events policy**.

At this point, SmartEvent Intro will begin to read logs and detect events.

To learn how to manage and fine-tune the system using the SmartEvent Intro Client, see the *SmartEvent Administration Guide* for your software version on the Check Point Support Center (http://supportcenter.checkpoint.com).

Creating a Consolidation Session for SmartReporter

The Consolidation session reads logs from the log server and adds them to the SmartReporter database.

- If there is a single log server in the environment, the Consolidation session is automatically created.
- If there is more than one log server, you must create the Consolidation session for each log server.

To create a Consolidation session:

1. In the **Selection Bar** view, select **Management > Consolidation**.
2. Select the **Sessions** tab.
3. Click **Create New** to create a new session.

   The **New Consolidation Session** window appears.
4. Select the log server from which logs will be collected and will be used to generate reports.
5. Click **Next**.

   The **New Consolidation Session** window appears.
6. Choose whether to use the default source logs and database tables, or select custom source logs and database tables for consolidation.

If you selected **Select default log files and database**, click **Finish** to complete the process. The source of the reports will be preselected logs. The report data will be stored in the default database table named CONNECTIONS. The preselected logs are the sequence of log files that are generated by Check Point products. The preselected logs session will begin at the beginning of the last file in the sequence, or at the point the sequence was stopped.

If you want to customize the Consolidation session refer to the *SmartReporter Administration Guide* for your software version on the Check Point Support Center (http://supportcenter.checkpoint.com).

Chapter 5

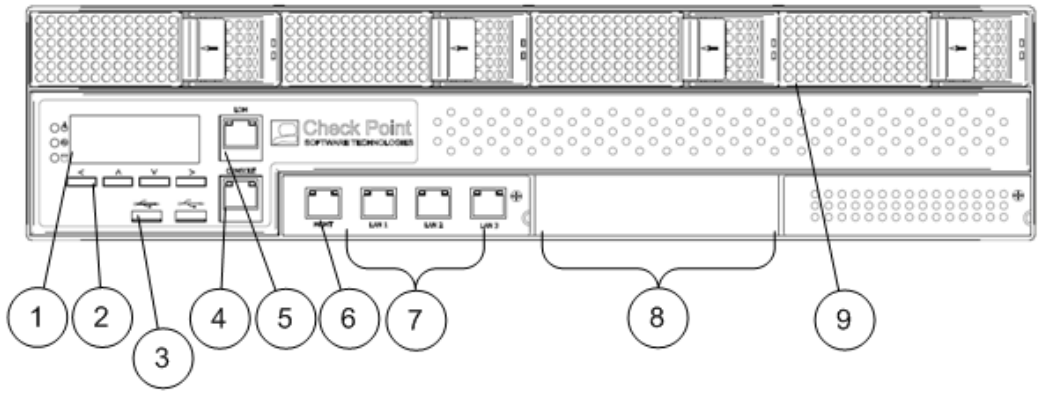
Smart-1 Hardware

This chapter provides instructions for installing and removing hardware components on the Smart-1 appliance.

In This Chapter

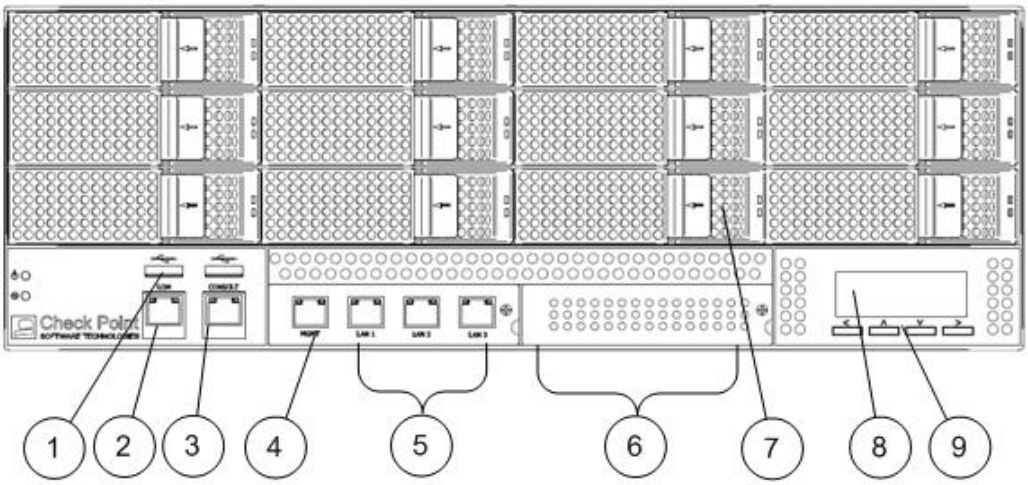
Smart-1 50 Front Panel	32
Smart-1 150 Front panel	33
LCD Display Screen	33
Customer Replaceable Parts	34

Smart-1 50 Front Panel



Key	Description
1	LCD display screen
2	Screen operation keys
3	USB ports
4	Console port - for a serial connection to the appliance using a terminal emulation program such as HyperTerminal
5	LOM (Lights-out Management) port
6	Management configuration port
7	Built-in ethernet ports (Lan1-Lan3)
8	slot for optional fiber channel SAN card. For setup instructions see sk43364 (http://supportcontent.checkpoint.com/solutions?id=sk43364)
9	4 hard disk drives

Smart-1 150 Front panel



Key	Description
1	USB ports
2	LOM (Lights-out Management) port
3	Console port - for a serial connection to the appliance using a terminal emulation program such as HyperTerminal
4	Management configuration port
5	Built-in ethernet ports (Lan1-Lan3)
6	Slot for optional fiber channel SAN card. For setup instructions see sk43364 (http://supportcontent.checkpoint.com/solutions?id=sk43364).
7	12 hard disk drives
8	LCD display screen
9	Screen operation keys

LCD Display Screen

Smart-1 appliances (other than Smart-1 25) have an LCD screen that can be used to perform basic management operations. The management IP address, netmask and default gateway of the Check Point appliance can be configured. The appliance can also be rebooted and shut down.

LCD Screen Operation Keys

To	Press
Enter the main menu	➤
Navigate within the menu	▲ or ▼
Select a menu option	➤
Go back to a previous menu	◄

Menu Options

Menu	Sub-menu	Purpose
Network		
	Set MGMT IP	Set the management interface's IP address
	Set Netmask	Set the management interface's network mask
	Set Default GW	Set the management interface's default gateway
System		
	Reboot	Reboot the appliance

When Entering an IP Address

To	Press
Move to the next digit	➤
Move back to the previous digit	➤
Approve the change	➤ when cursor is located on the last digit
Cancel the IP change	➤ when cursor is located on the first digit
Change current digit	▲ or ▼

Customer Replaceable Parts

To ensure maximum availability and ease of maintenance, the Smart-1 appliance contains the following customer replaceable parts:

- Smart-1 50:
  - Two power supplies
  - Four hard disk drives
  - Two cooling fans
- Smart-1 150:
  - Three power supplies
  - Up to twelve hard disk drives
  - Three cooling fans

Unless directed to do so by Check Point technical support, customers are prohibited by warranty and support agreements from replacing any parts. Customers are prohibited from opening the Smart-1 case under any circumstances.

Power Supplies

This section presents the procedures for removing and installing a power supply unit. It is not necessary to power off the appliance before adding or removing a power supply.

Removing the Power Supply

To remove a power supply unit:

1. If the power supply alarm sounds, press the red alarm button to the right of the power supply. This will stop the alarm.
2. Remove the power cord.
3. Loosen the retaining screw located above the power socket.
4. Pull the extraction handle to remove the power supply unit.

Note - Use only the extraction handle to remove the power supply unit. To prevent damaging the power supply, do not pull on the retaining screw, power cord clip or any other part of the unit.

Installing the Power Supply

To install a replacement power supply:

1. Insert the power supply into its slot and push firmly until it clicks into place.
2. Tighten the retaining screws.
3. Insert the power cord.

Hard Disk Drives

Smart-1 50 contains 4 hot-swappable redundant hard disk drives (RAID 10).

Smart-1 150 can contain up to 12 hot-swappable hard disk drives.

Implemented by a dedicated LSI Logic RAID controller, Smart-1 performs RAID10 mirroring and striping across all of the installed hard disk drives.

Use the **raidconfig** SecurePlatform command to perform basic maintenance and monitoring procedures on your Smart-1 RAID array.

raidconfig	
Description	Perform basic maintenance and monitoring procedures on the Smart-1 RAID array
Syntax	`raidconfig [status / rebuild /extendstorage / extendfs / alarmon / alarmoff]`

Parameters

Parameter	Description
`status`	Shows the status of RAID controllers and virtual disks
`rebuild`	Rebuilds degraded volumes. Use this option after replacing one or more disks in the RAID array, or if the `raidconfig status` command indicates a drive is not online.
`extendstorage`	Use if additional hard drives have been added to a Smart-1 150 machine. See detailed instructions below.
`extendfs`	Use if additional hard drives have been added to a Smart-1 150 machine but the proper RAID configuration has already been manually defined.
`alarmon`	Enables alarm sound.
`alarmoff`	Disables alarm sound.

Removing a Hard Drive

Any single hard disk can be safely removed without risking the integrity of the RAID array or compromising the data.

The hard disk drives are numbered 1-4 on Smart-1 50 from left to right, and 1-12 on Smart-1 150 from left to right, top to bottom. The upper left hard drive is #1, upper right hard drive is #4. On Smart-1 150 the lower right hard drive is #12.

Warning - When removing more than one hard drive, please DO NOT REMOVE both of the hard drives in the following pairs in order to maintain your RAID array integrity :

- In Smart-1 50, hard drives 1+2 or 3+4 should not be removed together.
- In Smart-1 150, also hard drives 5+6, 7+8, 9+10, or 11+12.

For example, you may replace hard disk drives 1+3 or disks 2+4.

To remove a hard disk drive:

1. Unlock the drive.
2. Slide the release latch toward the left.
3. Remove the drive from its slot.

Installing a Hard Disk Drive

To install a hard disk drive:

1. Slide the replacement hard disk drive into the slot.
2. Push the extraction handle until it closes and the drive clicks into place.
3. If the command `raidconfig status` shows that the new hard disk drive is not rebuilding, run the command `raidconfig rebuild` to initiate the rebuild of the RAID array on the new disk drive.

Smart-1 150 Raid Storage

Smart-1 150 can contain up to 12 hard drives. If the appliance has been purchased with less than 12 hard drives and you would like to add more storage capacity, follow the guidelines and instructions below.

RAID Storage Guidelines

- Additional hard drives should always be added in multiples of four - the appliance should always contain 4, 8 or 12 hard drives.
- For each group of 4 hard drives, the RAID controller creates a separate RAID 10 array. The initial setup is 4 hard drives configured in one RAID 10 array.
- When four additional hard drives are inserted, one additional RAID 10 array built of four hard drives will be added.
- When eight additional hard drives are inserted, two additional RAID 10 arrays, each built of four hard drives will be added.
- When less than four additional hard drives are inserted, storage will not be extended.
- When more than four but less than eight additional hard drives are inserted, storage will be extended using only four drives, i.e. only one additional four-hard-drive RAID 10 array will be added.
- Additional storage is always added to the `/dev/vg_splat/lv_log` logical volume.

Extending Appliance Storage

1. Disconnect the power from the appliance.
2. Insert the additional hard drives into the appliance according to the guidelines above.
3. Power on the appliance.
4. Wait for the boot process to finish.

5. Make sure that the additional hard drives have been inserted correctly and are recognized by the system by running the command
   `/sbin/raidconfig status`
6. Stop all Check Point processes by running `cpstop` or `mdsstop`
7. Stop all other processes that are using `/var/log`. To see a list of these processes, run `lsof /var/log`
8. Add the additional storage to the file system by running the command
   `/sbin/raidconfig extendstorage`

In the event that the storage extension process fails:

1. Run the command
   `/opt/MegaRAID/MegaCli/MegaCli –CfgForeign –Clear –a0`
2. Repeat steps 5 to 8 above.

Verifying Hard Drive Extension

1. Run the `/sbin/raidconfig status` command to view the status of the hard disk drives. Additional hard disk drives should appear configured in additional four discs' RAID 10 arrays.
2. Run the `lvdisplay /dev/vg_splat/lv_log` command. The additional storage should appear available under this logical volume.

Cooling Fans

The Smart-1 appliance contains three cooling fans. Each cooling fan operates independently of the other(s), providing redundancy in the event of failure.

This section presents the procedures for removing and installing a fan unit. It is not necessary to power off the appliance before adding or removing a fan unit.

Removing Fan Units

To remove a fan unit:

1. Loosen the retaining screws in the corners of the fan assembly.
2. Gently pull the fan unit out of the appliance.

Installing Fan Units

To install a fan unit:

1. Insert the fan unit into the appliance. Push firmly until it clicks into place.
2. Tighten the retaining screws in the corners of the fan assembly.

Chapter 6

Restoring Factory Defaults

You may restore the factory default images on the appliance using the WebUI, a console connection application (such as HyperTerminal) or the LCD panel.

Important - Restoring factory default images will delete all information on the appliance including images, backup files, and logs.

In This Chapter

Restoring Factory Defaults using the WebUI	38
Restoring Factory Defaults using the Console	38
Restoring Using the LCD Panel	39

Restoring Factory Defaults using the WebUI

Smart-1 contains a default factory image for Security Management server or Multi-Domain Security Management according to the Check Point license you have purchased. Choose the image that is applicable to your license.

To revert to an earlier image, in the Smart-1 WebUI:

1. Click **Appliance** > **Image Management**.
2. Select the relevant image version you wish to restore.
3. Click **Revert**.

Restoring Factory Defaults using the Console

The below procedure defines how to restore factory defaults using a terminal emulation program such as HyperTerminal.

1. Using the supplied serial console cable to the console port, connect Smart-1 to a HyperTerminal machine. In the **Port Settings** window, the setting for the Serial console is 9600 8N1 (9600 BPS, 8 bits, no parity, 1 stop bit). From the **Flow control** drop down menu, select **Hardware**.
2. Configure the hyperterminal parameters.
3. In **Hyperterminal**, click **Call** > **Call** to connect to the appliance.
4. Power on Smart-1.
5. While booting up, the following text appears: “Press any key to see the boot menu [booting in 4 seconds]”.

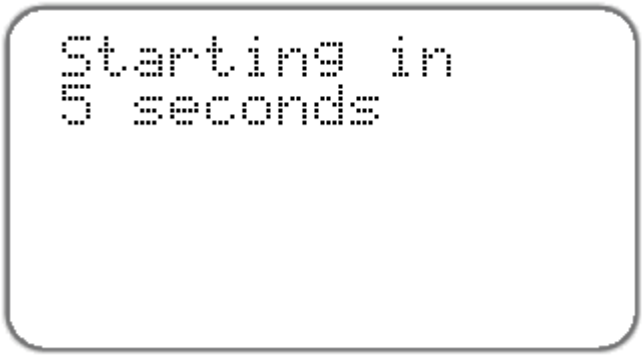
   There are approximately four seconds to press any key in order to bring up the boot grub menu. Once the boot grub menu is displayed, there will be approximately ten seconds to press any key or the machine will continue booting up.
6. Scroll down the grub menu to highlight **Reset to factory defaults**.

   Select the relevant default image version.
7. Press **Enter**.

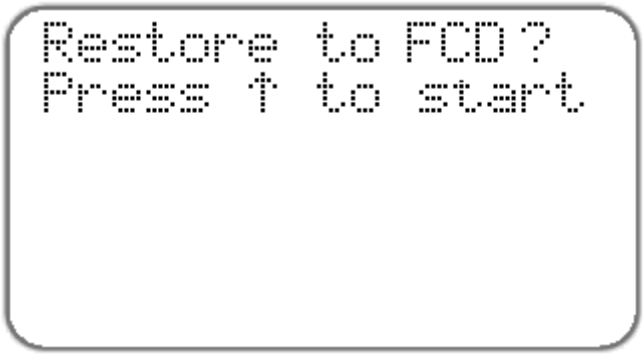
Restoring Using the LCD Panel

To restore the Smart-1 appliance to its default factory configuration using the LCD Panel keys:

1. Reboot or power on the appliance.
2. When the countdown begins, press any of the arrow keys.

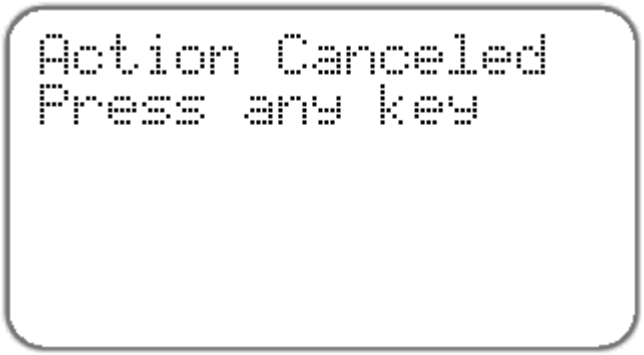


   The **Boot** menu appears.
3. Using the arrow buttons, scroll to the relevant option:
   - **Reset to SMC FCD** - for Security Management Server and then press the **UP** arrow.
   - **Reset to PV-1 FCD** - for Multi-Domain Security Management and then press the **UP** arrow.
4. Confirm the reset by pressing the **UP** arrow.



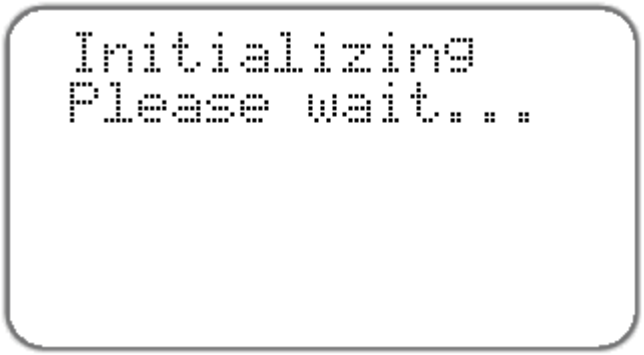
Important - All data on the appliance will be erased.

   Pressing any other key causes the **Action Canceled** message to appear:



   At this point, pressing any key returns you to the boot menu.
5. Once you have confirmed the reset, wait for the appliance to restore the factory image. While the appliance is restored to the Software Blades default image, a **Reverting image don't turn off** message displays continuously.

When the appliance has been restored to its default factory configuration, the appliance reboots and the **Initializing** message appears.



Chapter 7

Lights Out Management

This chapter discusses the Lights-Out Management (LOM) integrated card that is supplied with the Smart-1 50/150 appliance and basic configuration options.

In This Chapter

Introduction	41
Initial Login	41
Basic Configuration Options	42
Remotely Controlling the Appliance	42
Remotely Controlling the Power of the Appliance	42
Managing LOM Card Users	43
Configuring LOM Keyboard/mouse Settings	43
Configuring LOM Settings	44
Setting the Date and Time	44
Defining a LOM Login Message	44

Introduction

The Lights-Out Management (LOM) card enables you to remotely administer the appliance and perform maintenance operations.

The LOM card is configured by connecting to the LOM port through a Web interface. The basic configuration options of the LOM card are:

- Appliance Control - Remote lights-out power management. Turning the power ON or OFF, or resetting the appliance.
- LOM User Management - Managing LOM card user accounts.
- LOM Settings - Managing LOM IP settings.

This chapter describes the recommended procedures you can perform with the card.

Initial Login

1. Open a web browser and enter the default IP address of the LOM card: 192.168.0.100. The login page appears.
2. Login with the default User name (**admin**) and password (**admin**), all lower case. The LOM home page appears.

Note - Following 30 minutes of inactivity you will automatically be logged out.

Basic Configuration Options

The options in the main menu on the LOM home page enable you to access the following basic configuration options:

- Remotely control the appliance
- Remotely control the power of the appliance
- Manage LOM card users
- Configure LOM keyboard/mouse settings
- Configure LOM network settings
- Set date and time
- Define a LOM login message

Remotely Controlling the Appliance

The Appliance Control menu option enables you to access the appliance via a web interface (Java application). Prior to using this option, ensure that you have Java Runtime installed on the host machine.

To run the remote console:

1. Click the **Appliance Control** menu option.
2. Select **KVM Console** and then **Open Console**. A new window opens that enables you to remotely control the Smart-1 appliance.

Remotely Controlling the Power of the Appliance

Using the LOM card, it is possible to remotely switch ON the Smart-1 appliance even if the power is off, switch OFF the appliance, or reset the appliance.

Note - The main power switch at the rear of the appliance must be turned ON. If the switch is in the OFF position, remote power management is not possible.

To turn ON/OFF or reset the appliance:

1. Click the **Appliance Control** menu option.
2. Select **Power Control**, the relevant option and click **Apply Changes**.

Managing LOM Card Users

You can create, modify, and delete users. You can also assign privileges to users.

To create a user:

1. Click the LOM User Management menu option. The User Management page appears.
2. Select a row and click Create. The User Add dialog box appears.
3. Enter the following:
   - **User name**: a user name up to fourteen characters)
   - **Password**: a password for the login name. It must be at least 5 and no more than 14 characters long.
   - **Confirm Password**: confirm the password.
   - **Network Privileges**: assign the Administrator or Operator privileges according to the table below.

Network Privileges

	Administrator	Operator
Login	Yes	Yes
Enter KVM console	Yes	Yes
Create user	Yes	N/A
Modify user	Yes	N/A
Delete user	Yes	N/A
Date/time settings	Yes	Yes
Edit login message	Yes	N/A
Remote power management	Yes	Yes
Network setting	Yes	N/A
Keyboard/mouse setting	Yes	Yes

To modify a user:

1. Select an existing user from the list and click **Modify**. The User Modify dialog box appears.
2. Modify the fields as required.
3. To change the password, check the **Change Password** checkbox.
4. Click **Modify User** to apply the changes.

To delete a user:

1. Select an existing user from the list and click **Delete**. A message appears.
2. Click **OK**.

Configuring LOM Keyboard/mouse Settings

To use the remote console feature described above, specify the operating system that the host machine is running.

To configure keyboard/mouse settings:

1. Click the **KVM Settings** menu option.
2. Select the relevant option:
   - Absolute (for Windows)

- Relative (for Linux)

3. Click **Apply Changes**.

Configuring LOM Settings

The network settings option enables you to change the default IP address and other basic network settings of the LOM card.

To configure LOM network settings:

1. Click the **LOM Settings** menu option and select **Network**.
2. Select **Static** and enter the following values.
   - **IP address**: the IP address of the LOM.
   - **Subnet mask**: the subnet mask of the LOM's local network.
   - **Gateway IP address**: the Default Gateway IP address.
   - **Remote Console and HTTPS port**: port number on which the device's Remote Console server and HTTPS server are listening.

Setting the Date and Time

This option enables you to manually change the date and time of the LOM card.

Defining a LOM Login Message

This option enables you to define the login message that appears when accessing LOM via a browser.

To edit a login message:

1. Click the **Device Settings** menu option and select **Login Message**.
2. Enter the login message text.
3. Click **Apply Changes**.

Chapter 8

Registration and Support

In This Chapter

Registration	45
Support	45
Where to From Here?	45

Registration

Smart-1 requires a specific license to operate. Obtain a license and register (http://register.checkpoint.com/cpapp).

The MAC address required to obtain a license is found on the **Information** > **Appliance Status** page of the WebUI.

Support

For additional technical information about Check Point products, consult the Check Point Support Center (http://supportcenter.checkpoint.com).

Where to From Here?

You have now learned the basics that you need to get started. The next step is to obtain more advanced knowledge of your Check Point software.

See the relevant documentation for your software version on the Check Point Support Center:

Check Point documentation is available on the Check Point Support Center (http://supportcenter.checkpoint.com).

Be sure to also use the Online Help when you are working with the Check Point SmartConsole clients.